Victorian Government
Information Security

ISMF Implementation Check List

When implementing the revised ISMF, agencies should complete the following tasks:

No.	Task	Completed?
1	Update your governance arrangements: • Check that security governance arrangements, roles and responsibilities are current as defined in the ISM and PSPF. • Ensure your agency CIO & CISO are briefed, and have set the strategic direction.	
2	Review and update your mandatory ISMF document requirements as established in the VG Information Security Management (SEC POL 01). https://www.dtf.vic.gov.au/CA257310001D7FC4/pages/policies-and-standards-information-security-information-security-management-policy	
	Date of Compliance: Document updates for steps 4, 5 & 6 (below) must be completed by 30/06/2013	
3	Update your ICT Asset Register (see process in SEC GUIDE 01) • Ensure your agency's overall inventory of information assets is up to date and that significant information assets have been identified and recorded in an ICT assets inventory. • Update the ICT Asset Register with information provided by the Critical Information Infrastructure (CII) assessments, (Stream 2 of the DSLG 2.0 Program) • Note: DTF will run a CII workshop with each agency in the second half of 2012	
	Dates of Compliance: • The ICT asset Register is an ongoing internal process and should be updated accordingly • DTF will run a CII workshop with each agency in the second half of 2012 for a December report date.	

No.	Task	Completed?
4	Update your ICT Risk Assessment Report (see process in SEC GUIDE 01) • A Risk Assessment Report should already exist within the agency as a result of the previous VG SEC POL 01 requirements. • Identify existing documents required to support the update including the required security reports from any third parties, including ICT shared services providers and CII results. • As part of the Threat Consequence component of your risk assessment, ensure you have security classified your information assets as required by SEC STD 02 Information Security - Data classification and management (2009) and updated in March 2012 v1.5 with an addendum.	
5	Update your agency Information Security Policy • An Information Security Policy should already exist within the agency as a result of the previous VG SEC POL 01. • Review it in the light of the issues identified in the updated ICT Risk Assessment Report, changes to Victorian Government Policy and Standard and update it as required.	
6	Update your Incident Reporting Procedure • Update the existing agency Incident reporting process to include reporting to DSD CSOC • Establish an OnSecure account for relevant roles to be able to report incidents	
	Date of Compliance: Reporting to OnSecure takes effect as per ISMF Standard 01 and as incidents arise.	
7.1	Compliance Reporting Part One - AGD PSPF based self-assessment • AGD has published a PSPF self-assessment template to enable mandatory agency internal reporting. DTF has modified the template. • The 31 Mandatory Requirements encompass a broader scope than Information Security. The domains cover governance, physical, personal and information security. • Complete the PSPF self-assessment template and present it to senior executive and Audit & Risk Committee in draft at 16/11/12 and final version 30 May 2013. Then annually after that. • Forward a copy to DTF for aggregation and presentation to DSLG and SC&MC.	
	Date of Compliance: For FY 12/13, the Self-Assessment is a two-step process. Draft assessment 16 November 2012 and the formal assessment 30 May 2013; and thereafter an annual activity.	

No.	Task	Completed?
7.2	Compliance Reporting Part Two - Critical Information Infrastructure (CII) assessments, (Stream 2 of the DSLG 2.0 Program) • DTF will run a CII workshop with each agency in the second half of 2012. • The criteria used to identify CII assets are based upon the Victorian Government Business Impact Levels (see SEC GUIDE 02 Business Impact Levels and Other Criteria.) • The CII Health Check reports will be completed on each CII classified asset. • It is anticipated that some agencies will have no or very few CII classified assets • The CII Health Check Report should be presented to your Senior Executive and Audit and Risk Committee annually at 31 December, commencing 2012. • Forward a copy to DTF for aggregation and presentation to DSLG and SC&MC	
	Date of Compliance: DTF will run a CII workshop with each agency in the second half of 2012 for a December report date.	
8	Significant Information Asset Assessment Requirements • Your agency must complete the following mandatory assessment activities comprising the ISM mandated activities for all your Significant Information Assets (see definition in SEC STD 01 Information Security management) • Significant Information Assets must have a current System Risk Management Plan (SRMP), System Security Plan (SSP) and Standard Operating Procedures (SOPs) • These ISM defined assessment activities will document the risk treatment plans and associated costs • Risk treatment plans (including allocation of funding and implementation timeframes) are an agency decision and are to be formally signed off by the Agency Executive	
	Date of Compliance: Agencies that have a significant level of CII, may elect to address only their CII information assets in the first year of this requirement. In the subsequent years they must address all Significant Information Assets. Agency's must: • Maintain an annual schedule for the completion and update (every 2 years) of SRMP, SSP and SOPs for each Significant Information asset. • Forward a copy to DTF for aggregation and presentation to DSLG and SC&MC	